Subpart C—Communication (Port—Facility—Vessel)

§ 101.300 Preparedness communications.

(a) *Notification of MARSEC Level change.* The COTP will communicate any changes in the MARSEC Levels through a local Broadcast Notice to Mariners, an electronic means, if available, or as detailed in the AMS Plan.

(b) *Communication of threats.* When the COTP is made aware of a threat that may cause a transportation security incident, the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities in his or her AOR the following details:

(1) Geographic area potentially impacted by the probable threat;

(2) Any appropriate information identifying potential targets;

(3) Onset and expected duration of probable threat;

(4) Type of probable threat; and

(5) Required actions to minimize risk.

(c) *Attainment.* (1) Each owner or operator of a vessel or facility required to have a security plan under parts 104 or 105 of this subchapter affected by a change in the MARSEC Level must ensure confirmation to their local COTP the attainment of measures or actions described in their security plan and any other requirements imposed by the COTP that correspond with the MARSEC Level being imposed by the change.

(2) Each owner or operator of a facility required to have a security plan under part 106 of this subchapter affected by a change in the MARSEC Level must ensure confirmation to their cognizant District Commander the attainment of measures or actions described in their security plan and any other requirements imposed by the District Commander or COTP that correspond with the MARSEC Level being imposed by the change.

[USCG–2003–14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003]

§ 101.305 Reporting.

(a) *Notification of suspicious activities.* An owner or operator required to have a security plan under part 104, 105, or 106 of this subchapter shall, without delay, report activities that may result in a transportation security incident to the National Response Center at the following toll free telephone: 1–800–424–8802, direct telephone: 202–267–2675, fax: 202–267–2165, TDD: 202–267–4477, or use the NRC Web Reporting function located on the NRC Web Site: *http://www.nrc.uscg.mil/.* Any other person or entity is also encouraged to report activities that may result in a transportation security incident to the National Response Center.

(b) *Notification of breaches of security.* An owner or operator required to have a security plan under parts 104, 105, or 106 of this subchapter shall, without delay, report breaches of security to the National Response Center via one of the means listed in paragraph (a) of this section.

(c) *Notification of transportation security incident (TSI).* (1) Any owner or operator required to have a security plan under part 104 or 105 of this subchapter shall, without delay, report a TSI to their local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(2) Any owner or operator required to have a security plan under part 106 of this subchapter shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(d) Callers to the National Response Center should be prepared to provide as much of the following information as possible:

(1) Their own name and contact information;

(2) The name and contact information of the suspicious or responsible party;

(3) The location of the incident, as specifically as possible; and

(4) The description of the incident or activity involved.

[USCG–2003–14792, 68 FR 39278, July 1, 2003, as amended by USCG–2004–18057, 69 FR 34925, June 23, 2004]

§ 101.310 Additional communication devices.

(a) *Alert Systems.* Alert systems, such as the ship security alert system required in SOLAS Chapter XI–2, Regulation 6 (Incorporated by reference, see § 101.115), may be used to augment communication and may be one of the communication methods listed in a vessel or facility security plan under part 104, 105, or 106 of this subchapter.

(b) *Automated Identification Systems (AIS).* AIS may be used to augment communication, and may be one of the communication methods listed in a vessel security plan under part 104 of this subchapter. See 33 CFR part 164 for additional information on AIS device requirements.

Subpart D—Control Measures for Security

§ 101.400 Enforcement.

(a) The rules and regulations in this subchapter are enforced by the COTP under the supervision and general direction of the District Commander, Area Commander, and the Commandant. All authority and power vested in the COTP by the rules and regulations in this subchapter is also vested in, and may be exercised by, the District Commander, Area Commander, and the Commandant.

(b) The COTP, District Commander, Area Commander, or Commandant may assign the enforcement authority described in paragraph (a) of this section to any other officer or petty officer of the Coast Guard or other designees authorized by the Commandant.

(c) The provisions in this subchapter do not limit the powers conferred upon Coast Guard commissioned, warrant, or petty officers by any other law or regulation, including but not limited to 33 CFR parts 6, 160, and 165.

§ 101.405 Maritime Security (MARSEC) Directives.

(a)(1) When the Coast Guard determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against the maritime elements of the national transportation system, the Coast Guard may issue a MARSEC Directive setting forth mandatory measures. Only the Commandant or his/her delegee may issue MARSEC Directives under this section. Prior to issuing a MARSEC Directive, the Commandant or his/her delegee will consult with those Federal agencies having an interest in the subject matter of that MARSEC Directive. All MARSEC Directives issued under this section shall be marked as sensitive security information (SSI) in accordance with 49 CFR part 1520.

(2) When a MARSEC Directive is issued, the Coast Guard will immediately publish a notice in the FEDERAL REGISTER, and affected owners and operators will need to go to their local COTP or cognizant District Commander to acquire a copy of the MARSEC Directive. COTPs and District Commanders will require owners or operators to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information.

(b) Each owner or operator of a vessel or facility to whom a MARSEC Directive applies is required to comply with the relevant instructions contained in a MARSEC Directive issued under this section within the time prescribed by that MARSEC Directive.

(c) Each owner or operator of a vessel or facility required to have a security plan under parts 104, 105 or 106 of this subchapter that receives a MARSEC Directive must:

(1) Within the time prescribed in the MARSEC Directive, acknowledge receipt of the MARSEC Directive to their local COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander; and

(2) Within the time prescribed in the MARSEC Directive, specify the method by which the measures in the MARSEC Directive have been implemented (or will be implemented, if the MARSEC Directive is not yet effective).